UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,574	02/27/2004	Matthew P. Chant	LOT920040002 (044)	7947

46321 7590 01/28/2011

CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 2022
BOCA RATON, FL 33487

EXAMINER	
CHANG, JUNGWON	
ART UNIT	PAPER NUMBER
2454	

MAIL DATE	DELIVERY MODE
01/28/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/789,574
Filing Date: February 27, 2004
Appellant(s): CHANT ET AL.

Steven M. Greenberg
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 9/27/10 appealing from the Office action mailed 4/17/08.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1 through 20 are pending in this Application and have been twice rejected.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal.

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

7,206,814	**Kirsch**	**4-2007**
7,127,741	**Bandini et al.**	**10-2006**
7,224,778	**Aoki**	**5-2007**

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-9 and 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch (US 7,206,814), in view of Bandini et al, (US 7,127,741), hereinafter Bandini.

3. As to claim 1, Kirsch discloses the invention as claimed, including a method for classifying electronic mail message transfer requests for policy enforcement (col. 2, lines 54-64, "categorize received e-mail messages") comprising the steps of:

identifying a source of an incoming electronic message (col. 2, lines 54-64,

"sender could be identified by an email address, a single IP address");

classifying said source (fig. 2, "whitelist, blacklist, unsolicited email"; col. 2, lines 54-64, "categorize received e-mail messages based on information about the sender"); and,

applying the message transfer policy to said incoming electronic message (fig. 2; col. 5, line 60 – col. 6, line 40, "if the sender is on the whitelist, the message is passed on to the recipient…if the sender is on a blacklist…the message will not accepted…").

4. Kirsch explicitly discloses a policy (deleting message, sending message to a spam folder, delivering message) that is used to determine how to process the incoming message based on the classification of the source (whitelist, blacklist, good reputation, bad reputation). If the source is on the whitelist (trusted classification), the message transfer policy is selected for the trusted source (Kirsch; send to recipient; 104, fig. 2; col. 5, line 60 - col. 6, line 9; col. 8, line 63 - col. 9, line 31). And if the source is on the blacklist (untrusted classification), the message transfer policy is selected for the untrusted source (delete the message; send the message to a spam folder; 116, 108, fig. 2; col. 17, line 53 - col. 18, line 4). Kirsch's deleting message, sending the message to a spam folder or delivering message is equivalent to the claimed "message transfer policy". Therefore, Kirsch discloses message transfer policy is selected based upon the classification (col. 5, line 60 - col. 6, line 9; col. 8, line 63 - col. 9, line 31; col. 17, line 53 - col. 18, line 4).

Bandini, on the other hand, more explicitly discloses a message transfer policy is

selected based upon the classification (214, 216, fig. 2; figs. 3, 4; col. 5, lines 14-43, "policy engine 214 accepts message from SMTP relay module 202 and determines which policies are applicable to a message by building a list 302 of sender policies for the sender, source 204 of the message"; col. 5, lines 61-67, "access control policies such as destinations to which email is prohibited from being sent, or sources from which email cannot be received"). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Kirsch and Bandini because Bandini's teaching would allow the mail system easy to process the incoming messages, as taught by Bandini (col. 5, lines 14-67).

5. As to claim 2, Kirsch discloses wherein said identifying step comprises the step of identifying a network address for said source (col. 2, lines 54-64, "sender could be identified by an email address, a single IP address").

6. As to claims 3 and 4, Kirsch discloses wherein said classifying step comprises the step of classifying said source as one of a trusted source, a blocked source, and a suspect source (col. 5, line 60 – col. 6, line 40, "sender is on the whitelist... sender is on a blacklist").

7. As to claim 5, Kirsch discloses wherein said classifying step further comprises the step of classifying said source as a blocked source where said source appears in a realtime black hole list (col. 5, line 60 – col. 6, line 40, "sender is on a blacklist").

8. As to claim 6, Kirsch discloses wherein said classifying step further comprises the step of classifying said source as a suspect source where said source appears in a realtime black hole list (col. 13, lines 31-56, "new sender is placed...as suspected spam folder").

9. As to claim 7, Kirsch discloses classifying said source as an authenticated source only where an authenticated connection has been established with said source (col. 6, line 59 – col. 7, line 19; col. 9, lines 20-31, "the sender has a good reputation, in which case the message will be passed"; col. 17, lines 46-52, "message is passed only if the final IP address, final domain name, or IP path have never been used to pass unwanted messages").

10. As to claim 8, Kirsch discloses wherein said applying step comprises the step of limiting transfer of messages from a source classified as suspect (col. 13, lines 51-56, "new sender is placed...as suspected spam folder").

11. As to claim 9, Kirsch discloses wherein said applying step comprises the step of limiting transfer of messages from a source classified as anonymous (col. 13, lines 31-56, "unknown senders").

12. As to claim 12, it is rejected for the same reasons set forth in claim 1 above In

addition, Kirsch discloses a machine readable storage having stored thereon a computer program (col. 3, line 62 – col. 4, line 65, "server is running software 26 for handling e-mail messages").

13. As to claim 13, it is rejected for the same reasons set forth in claim 2 above.

14. As to claim 14, it is rejected for the same reasons set forth in claim 3 above.

15. As to claim 15, it is rejected for the same reasons set forth in claim 4 above.

16. As to claim 16, it is rejected for the same reasons set forth in claim 5 above.

17. As to claim 17, it is rejected for the same reasons set forth in claim 6 above.

18. As to claim 18, it is rejected for the same reasons set forth in claim 7 above.

19. As to claim 19, it is rejected for the same reasons set forth in claim 8 above.

20. As to claim 20, it is rejected for the same reasons set forth in claim 9 above.

21. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aoki (US 7,224,778), in view of Bandini et al, (US 7,127,741), hereinafter Bandini.

22. As to claim 10, Aoki discloses a system for classifying electronic mail message transfer requests for policy enforcement (fig. 2) comprising:

a mail server (22, fig. 1);

a set of mail transfer policies, each policy having an association with a corresponding source classification (fig. 2, "rule database to screen incoming messages, approved ID code, approved sender address"; col. 5, line 40 – col. 6, line 3);

at least one table of source identities having a particular classification (38, 39, fig. 1, "sender name, ID code name, source address, user address"; 60, 62, 112, fig. 2; col. 1, lines 32-47, "parameters stored in a database to block certain messages from unauthorized sources"; col. 5, lines 27-39, "a listing of approved message source is maintained"); and

a classifier (32, fig. 1; col. 5, lines 11-26, "filtering agent") coupled to said mail server (22, fig. 1) and said at least one table (38, 40, 42, fig. 1), said classifier identifying a source of an incoming electronic message in the mail server, classifying said source with a classification in the at least one table, and applying the one of the mail transfer policies to said incoming electronic message (col. 5, line 11 – col. 6, line 3, "filtering agent to inspect each selected message...rules database 40 are used by the subscription manager 32 to screen out as many unauthorized broadcast messages...and prevent their delivery").

23. Aoki explicitly discloses a policy (blocking message, refusing to accept message,

forwarding message) that is used to select based on the classification of the source (authorized sender, unauthorized sender). If the source is an authorized sender, and the message transfer policy is selected for the trusted source (66, fig. 2, "OK to forward message"; 108, fig. 3). And if the source is an unauthorized sender, the message transfer policy is selected for the untrusted source (64, fig. 2, "block message"; 110, fig. 3, "refuse to accept the message"). Aoki's blocking message, refusing to accept message, forwarding message is corresponding to the claimed "message transfer policy". Therefore, Aoki teaches selecting a message transfer policy based upon the classification (col. 1, lines 43-47, "the incoming messages are monitored…to block certain messages from unauthorized sources and forward authorized messages to an addressee"; col. 5, lines 40-52, "blocked 64 from delivery to its intended destination"; col. 5, lines 52 - col. 6, line 3, "messages may be forwarded directly to the destination user address"; col. 6, lines 4-26).

Bandini, on the other hand, more explicitly discloses message transfer policy is selected based upon the classification (214, 216, fig. 2; figs. 3, 4; col. 5, lines 14-43, "policy engine 214 accepts message from SMTP relay module 202 and determines which policies are applicable to a message by building a list 302 of sender policies for the sender, source 204 of the message"; col. 5, lines 61-67, "access control policies such as destinations to which email is prohibited from being sent, or sources from which email cannot be received"). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Aoki and Bandini because Bandini's teaching would allow the mail system easy to process the incoming

messages, as taught by Bandini (col. 5, lines 14-67).

24. As to claim 11, Aoki discloses wherein said at least one table comprises at least one table selected from the group consisting of a table of trusted sources, a table of authenticated sources, a table of suspect sources, a table of blocked sources, and a realtime black hole list (38, 39, fig. 1; 60, 62, 112, fig. 2; col. 1, lines 32-47, "parameters stored in a database to block certain messages from unauthorized sources"; col. 5, lines 27-39, "a listing of approved message source is maintained").

(10) Response to Argument

(A) The Rejection of claims 1 through 9 and 12 through 20 under 35 U.S.C. 103(a)

(1) Appellant argues that the deficiencies of Kirsch for the teachings of "selecting a message transfer policy based upon the classification".

The examiner respectfully disagrees. The specification of the present application defines the term "message transfer policy" in paragraph [0015], which states in part:

> ***A policy*** associated with the classification can be ***used to determine how to process the incoming message***. For instance, at one extreme a policy can indicate that all messages associated with a trusted classification are to be delivered, while at another extreme, a policy can indicate that all messages associated with a blocked classification are never to be delivered, in this way, spam can be intelligently handled uniformly and automatically without regard to the varying nature of disparate electronic mail clients.

Kirsch explicitly discloses a message transfer policy (deleting message, sending message to a spam folder, delivering message) that is used to determine how to process the incoming message based on the classification of the source (whitelist,

blacklist, good reputation, bad reputation). If the source is on the whitelist (trusted classification), the message transfer policy is selected for the trusted source (Kirsch; send to recipient; 104, fig. 2; col. 5, line 60 - col. 6, line 9; col. 8, line 63 - col. 9, line 31). And if the source is on the blacklist (untrusted classification), the message transfer policy is selected for the untrusted source (delete the message; send the message to a spam folder; 116, 108, fig. 2; col. 17, line 53 - col. 18, line 4).

Kirsch's deleting message, sending the message to a spam folder or delivering message is equivalent to the claimed "message transfer policy". Therefore, Kirsch discloses message transfer policy is selected based upon the classification (col. 5, line 60 - col. 6, line 9; col. 8, line 63 - col. 9, line 31; col. 17, line 53 - col. 18, line 4).

In addition, Bandini discloses selecting a message transfer policy based upon the classification (214, 216, fig. 2; figs. 3, 4; col. 5, lines 14-43, "policy engine 214 accepts message from SMTP relay module 202 and determines which policies are applicable to a message by building a list 302 of sender policies for the sender, source 204 of the message"; col. 5, lines 61-67, "access control policies such as destinations to which email is prohibited from being sent, or sources from which email cannot be received").

(B) The Rejection of claims 10 through 11 under 35 U.S.C. 103(a)

(1) Appellant argues that the deficiencies of Aoki for the teachings of "selecting a message transfer policy based upon the classification".

The examiner respectfully disagrees. Similar to Kirsch's reference, Aoki explicitly discloses a policy (blocking message, refusing to accept, forwarding message) that is

used to select based on the classification of the source (authorized sender, unauthorized sender). If the source is an authorized sender, and the message transfer policy is selected for the trusted source (66, fig. 2, "OK to forward message"; 108, fig. 3). And if the source is an unauthorized sender, the message transfer policy is selected for the untrusted source (64, fig. 2, "block message"; 110, fig. 3, "refuse to accept the message").

Aoki's blocking message, refusing to accept message, forwarding message is corresponding to the claimed "message transfer policy". Therefore, Aoki teaches selecting a message transfer policy based upon the classification (col. 1, lines 43-47, "the incoming messages are monitored...to ***block certain messages from unauthorized sources and forward authorized messages to an addressee***"; col. 5, lines 40-52, "***blocked 64 from delivery to its intended destination***"; col. 5, lines 52 - col. 6, line 3, "messages may be ***forwarded directly to the destination user address***"; col. 6, lines 4-26).

In addition, Bandini discloses selecting a message transfer policy based upon the classification (214, 216, fig. 2; figs. 3, 4; col. 5, lines 14-43, "policy engine 214 accepts message from SMTP relay module 202 and determines which policies are applicable to a message by building a list 302 of sender policies for the sender, source 204 of the message"; col. 5, lines 61-67, "access control policies such as destinations to which email is prohibited from being sent, or sources from which email cannot be received").

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/JUNGWON CHANG/
Primary Examiner, Art Unit 2454

Conferees:

/Joseph E. Avellino/

Supervisory Patent Examiner, Art Unit 2454

/Larry Donaghue/

Primary Examiner, Art Unit 2454